International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 4, pp: (201-204), Month: October - December 2015, Available at: www.researchpublish.com

Global Wireless E-Voting

[1]Ashish Ramteke, [2]Dr. D. V. Rojatkar

[1]B.E. student, [2]Supervisor, HOD, Electronics and Telecommunication dept. Government College of Engineering Chandrapur, India

Abstract: **In present voting system there is many problem related to the voting system so it becomes highly unsecured. In present electronic voting machine the person who came for the voting cannot be determined is it eligible voter or not. That mean the in charge officer is the main leader to handle the voting machine. Due to the vote count present in machine itself anybody can increase the vote count in present voting machine. In proposed machine that is "Global Wireless E-Voting" machine we can determine the eligibility of the voter by scanning the eye pattern and also the vote count is not kept into the same machine itself instead of it is store in the remote server by converting it into radio waves. Here anybody cannotincreasing the vote count of machine. Even in case of damage to voting machine there will not be any problem to continuity of the election process. The overall concept of "Global Wireless E-Voting "is explained.**

Keywords: **Interface device, LCD, Retina scanner.**

1. INTRODUCTION

The aim of project is to integrate an electronic voting scheme by using eye retina scanner.

In India voting is an important part of democracy. Voting system is the vital process in India. So to make it efficient and secured in the vision of modern technology we are "Global Wireless EVoting".

Why we are looking for it?

2. PRESENT SYSTEM

Since latest voting system is totally replaced by electronic machine to carry out voting. Now in a present system each and every section is given an electronic voting machine which stores the votes of the people how have voted for the particular candidate. The whole control is kept on the hand of In charge officer. Eligibility of the candidates can be checked by the In charge officer and allow for the voting. Finally we receive all the voting machine at a place and go for counting.

3. DISADVANTAGES OF THE PRESENT VOTING SYSTEM

After voting if any technical problems or damage created by machines it may leads to the reflection. The machine is unable to recognize the eligibility of a candidate, so the corrupted officers may misguide the people. Voting count can be increased by corrupted officers. During transportation of the machines the in charge person can change the status of machines and even may destroy.

This system is not a cost effective one. Since we need security, in charge officers, secured place for counting. The person from any other region cannot vote in for a candidate of other region. The voting is possible where the machine is located.

4. PROPOSED SYSTEM

In our system we are trying to keep counting of votes in to a remote secured system. In this system we are using a electronic circuit which enable the voter to vote and transfer this vote to the remote system by converting it to radio wave through the mobile towers. The person who came for voting is eligible or not checked by machine itself, Corruption is

eliminated by using this process. So automatically corruption may under controlled. This machine totally change the thinking of man. Machine itself can detect the eligibility of candidate. Even if the machine is damaged we need not to go for re election. A person even can vote from INTERNET and also from mobile system. We can vote from anywhere even though being a voter of another region.

5. EYE RETINA SCANNIG

The eye retina machine is a simple web cam which can capture the images effectively. The capture image will be represented in the form of a matrix where each pixel reprisenot24-bit (RGB, 8+8+8 format).

6. INTERFACE DEVICE

This is an electronic circuit which converts the input digital signals such as (retina pattern votes+ secure bits) to radio waves.

7. WORKING OF WHOLE SYSTEM

Whenever voters came for voting booth then he will be suggested to directly look at retina scanning machine at this time the machine scans the retina. Once retina scanning accepted then it sent signal to the voting machine as to accept the vote it will be powered on .then voter is made to vote. Now the whole data including the retina pattern is sent to interfacing device which is convert into radio waves of mobile frequency range and these radio waves are sent to mobile tower and then to the remote server, where the authentication and voters identification is stored into a secured database. The output data is first converted into digital pattern from the radio waves through the interface device kept the server side, and then retina pattern and vote separated. Next the retina pattern is compare against the existing database. If match is found then flag is check which indicates its voting status i.e. if the voter is not voted yet then positive ask is send to the mobile tower and then to the corresponding voting machine. This ack is recognized by the receiver kept at the voter side and machine is made to scan next retina pattern and vote, otherwise if–ve ack then alert alarm is made to ring.

8. HURDLES IN THE PATH OF IMPLEMENTATION

There are several more issues that we have to consider along the Implementation such as

- Security
- Efficiency
- Geographical Problems

8.1 SECURITY:

The radio waves of a mobile frequency consist of Retina pattern and vote can be generated by means of external source. To avoid this problemwe need to provide some set of security. We get some idea to solve this problem by using CDMA and another technique is inserting security bits at regular interval of time during the transmission of radio waves (Ex.2 msec) .At the server side after the given interval (2 msec) security bits are checked. In case of positive confirmation we can accept as valid vote, otherwise simply rejected.

Other problem is that one may trap the radio waves in between and can determine the person and the vote. This may disclose the result of the election before the completion of the voting process. To avoid this problem we can go for applying the efficient and complex encryption algorithm so that the transparency of data can be hidden and the server side the encrypted data can be again decrypted and original data can retrieved this make the trapping of wave meaningless. The encryption algorithm can be termed as Key Complex Algorithm, which is as follows,

- First it finds the length of the string.
- Generate the random numbers equal to the length of the string.
- Add the corresponding Characters from the given string and random values.

E.g. KSHITIJ

Let this be the given words.

The length of the given string is 7. So let us generate the 7 random numbers .Let numbers be

A) 8 12 34 4 11 9 26.

The ASCII values for KSHITIJ are

K S H I T I J

B) 75 83 72 73 84 73 74

Add corresponding A) and B) values as

8+75 12+83 34+72 4+73 11+84 9+73 26+74

83 95 106 77 95 82 100

The corresponding ASCII characters for these are

S _ j M _ R d

The corresponding characters for random values

א Ѽ θ ♥ ♦↔Ψ

Finally encrypted data as

S א _ Ѽ j θ M _ ♥ R ↔ d Ψ

The final encrypted data is formed in such a way that the random data at the even place and rest at odd place. This makes Decryption very easy. Simply subtract the character at even place from odd place character.

8.2 EFFICIENCY:

Whenever the data which is sent from the voter (client) side, it is in the large amount, this delays a bit a voting system and the data that is received at server side is in the multiple access mode i.e. more than one client is sending the data. To overcome this problem the following

Applying compression Algorithms at the Client and server side so those to decrease the data transfer. Compression technique such as JPEG compression or any other Compression. Instead of using single server PC we will go for distributed Operating system environment with multiple servers. This makes the job sharing and processing faster which leads to fast responds in case of Multiple Access Environment. To solve the concurrency problem in case of multiple access environments we will use CDMA technique which is as follow

Here the key values are orthogonal to each other i.e. k1*K2=0 and k1*k1=1 i.e. if any tries to decode the information with any other key the data will be vanished as the data will be in the form d1*k1.If you try to decode with K2 then effect will be as d1*k1*k2=0. This will vanish the data. And if correct decoding key i.e k1 is used then decoding will be d1*k1*k1=d1. This decodes the data correctly. As per the controlling concurrency for multiple access the data from all the nodes is accepted as k1*d1+k2*d2+k3*d3+k4*d4. In this case if you want the data corresponding to the second node then simply multiply the whole equation with the k2. This will give d2 as (k1*d1+K2*d2+k3*d3+k4*d4)*K2=d2. So by this we can show that any numbers of nodes are allowed to send the data, the server will accept all the data and which ever has to be extracted will be just multiplied with corresponding key. This gets the corresponding data. Hence the concept of Multiple access.

8.3 GEOGRAPHICAL PROBLEMS:

This is the problem regarding the area where technical facilities like mobile tower or Internet service is not present. In this case will convert the vote and retina pattern into the electrical information and pass it through the electrical conductors until we can reach the area where the technical facilities like internet or mobile tower is available, and if only internet facility is available is then we can convert this electrical information to digital means and with these data using computers connected to internet we can pass the vote and retina pattern. Here the eye scanner will be web cam.

9. FUTURE ENHANCEMENTS

This project can make look better to work over the mobiles that is voting is made possible through the mobile through SMS. This machine can be made vote through the INTERNET.

10. CONCLUSION

Thus this machine can be used for any level voting purpose. The machine provides high level of security, authentication, reliability, and corruption free mechanism.

By this we can get result with in minute after a completion of voting. Minimum manpower Utilization, hence mechanism is error free.

REFERENCES

[1] David Chaum. Secret-ballot receipts: True voter-verifiable elections, 2004.

[2] R. Mercuri. Explanation of voter-verified ballot systems. ACM Software EngineeringNotes (SIGSOFT), 27(5). Also at http://catless.ncl.ac.uk/Risks/22.17.html.

[3] A. PRosser, R. Kofler, R. Krimmer, and M. K. Unger. Security assets in e-voting. In the International Workshop on Electronic Voting in Europe, 2004.

[4] B. Var Acker. Remote e-voting and coercion: a risk assessmentmodel and solutions. In the International Workshop on Electronic Voting in Europe, 2004.

[5] T. Kohno, A. Stubblefield, A.D. Rubin, and D.S.Wallach. Analysis of an electronic voting system, 2004.